The Software Alliance

BSA

แนวทางปฏิบัติที่ดีระดับโลกสำหรับการคุ้มครองความเป็นส่วนตัว

บีเอสเอ คือ สมาคมชั้นนำที่ทำหน้าที่รณรงค์ส่งเสริมการเติบโตของอุตสาหกรรมซอฟต์แวร์ทั่วโลก มีสมาชิกเป็นบริษัทผู้นำในระดับแนวหน้าด้านการพัฒนานวัตกรรมเทคโนโลยีอันล้ำสมัย เช่น คลาวด์คอมพิวติ้ง (Cloud Computing) นวัตกรรมการใช้เทคโนโลยีเพื่อวิเคราะห์ข้อมูล (Data Analytics) และปัญญาประดิษฐ์ (Artificial Intelligence) การทำงานของนวัตกรรมเทคโนโลยีที่ใช้ซอฟต์แวร์เป็นตัวขับเคลื่อนต้องอาศัยข้อมูลที่เพิ่มมากขึ้น และในบางกรณีต้องใช้ข้อมูลส่วนบุคคล ดังนั้นสมาชิกของบีเอสเอจึงให้ความสำคัญสูงสุดกับเรื่องการคุ้มครองข้อมูลส่วนบุคคล และเราตระหนักว่าเรื่องนี้เป็นส่วนสำคัญของการสร้างความเชื่อมั่นของผู้บริโภคผู้ใช้นวัตกรรมเทคโนโลยีดังกล่าว

บีเอสเอจึงส่งเสริมแนวทางสำหรับการคุ้มครองความเป็นส่วนตัวที่ให้ความสำคัญแก่ผู้ใช้งานเป็นหลัก แนวทางที่ทำให้ผู้บริโภคมีกลไกสำหรับการควบคุมข้อมูลส่วนบุคคลของพวกเขา บีเอสเอยังสนับสนุนกรอบการทำงานด้านการคุ้มครองข้อมูล ที่ทำให้ยืนยันได้ว่าการใช้ข้อมูลส่วนบุคคลสอดคล้องกับความคาดหวังของผู้บริโภค ในขณะเดียวกันยังช่วยให้องค์กรธุรกิจสามารถดำเนินงานเพื่อผลประโยชน์ทางธุรกิจที่ชอบด้วยกฎหมาย

ในขณะที่ประเทศต่างๆ ทั่วโลก พิจารณาเรื่องการพัฒนากรอบการทำงานด้านการคุ้มครองข้อมูล มีหลายประเทศได้พยายามกำหนดแนวทางปฏิบัติที่ดีสำหรับเรื่องนี้ บีเอสเอสนับสนุนการใช้แนวทางปฏิบัติที่ดี ที่ส่งเสริมความโปร่งใสในการเก็บและใช้ข้อมูลส่วนบุคคล ช่วยให้มีทางเลือกบนพื้นฐานของข้อมูลที่เพียงพอและการเคารพในทางเลือกดังกล่าว โดยแนวทางปฏิบัติที่ดีต้องจัดให้มีการกำกับดูแลในเรื่องการเก็บและใช้ข้อมูลส่วนบุคคล ทำให้ผู้บริโภคสามารถควบคุมข้อมูลส่วนบุคคลของตนเองได้ จัดให้มีการรักษาความปลอดภัยที่มีประสิทธิภาพ และส่งเสริมการใช้ข้อมูลเพื่อวัตถุประสงค์ทางธุรกิจที่ชอบด้วยกฎหมาย **เราให้ความสำคัญกับแนวทางปฏิบัติที่ดีดังต่อไปนี้ เพื่อโอกาสที่จะบรรลุเป้าหมายดังกล่าว และเพื่อเป็นหลักนำทางที่เป็นประโยชน์สำหรับการพัฒนาและการปรับเปลี่ยนกรอบการทำงานด้านการคุ้มครองข้อมูลทั่วโลก**

ประเด็นพิจารณา	แนวทางปฏิบัติที่ดี
ขอบเขตของพื้นที่	กรอบการทำงานด้านการคุ้มครองข้อมูลควรใช้กำกับดูแลวิธีปฏิบัติที่มีความเชื่อมโยงอย่างใกล้ชิดเพียงพอกับประเทศแต่ละประเทศ กฎหมายควรใช้บังคับ (1) ในกรณีที่มีการกำหนดให้พลเมืองของประเทศเป็นเป้าหมายของการบังคับใช้กฎหมายอย่างเฉพาะเจาะจง (2) ในกรณีที่มีการเก็บข้อมูลส่วนบุคคลตามวัตถุประสงค์สำหรับการประมวลผลจากเจ้าของข้อมูลส่วนบุคคลในประเทศ ในขณะที่มีการเก็บข้อมูลส่วนบุคคล และ (3) ในกรณีที่การเก็บข้อมูลส่วนบุคคล ได้รับการดำเนินการโดยองค์กรที่ก่อตั้งขึ้นภายในประเทศผ่านการจัดการเพื่อให้การดำเนินกิจกรรมเกิดขึ้นได้จริงและมีประสิทธิภาพ
คำนิยามของข้อมูลส่วนบุคคล	ขอบเขตของข้อมูลที่รวมอยู่ในคำนิยามของข้อมูลส่วนบุคคล ควรเป็นข้อมูลที่เกี่ยวข้องกับผู้บริโภคที่มีการระบุตัวตนหรือสามารถระบุตัวตนได้ ผู้บริโภคที่สามารถระบุตัวตนได้ ไม่ว่าจะทางตรงหรือทางอ้อม ด้วยวิธีการที่สมเหตุสมผล จากการอ้างอิงกับแหล่งที่มา เช่น ชื่อผู้บริโภค หมายเลขประจำตัว ข้อมูลตำแหน่งที่ตั้ง และตัวระบุทางออนไลน์ หรือปัจจัยอย่างน้อยหนึ่งปัจจัยที่เจาะจงลักษณะทางกายภาพ สรีระ หรือพันธุกรรมของผู้บริโภค ขอบเขตของข้อมูลที่รวมอยู่ในคำนิยามนี้ควรเกี่ยวข้องกับข้อมูลส่วนบุคคล ซึ่งหากมีการจัดการผิดพลาดอาจจะส่งผลกระทบอย่างมีนัยสำคัญต่อความเป็นส่วนตัวของผู้บริโภค ข้อมูลที่มีการลบการระบุตัวตนแล้วด้วยมาตรการทางเทคนิคและมาตรการขององค์กรที่มีประสิทธิภาพเพื่อลดความเสี่ยงที่จะเกิดการระบุตัวตนใหม่ได้ ไม่ควรถือว่าเป็นข้อมูลที่รวมอยู่ในคำนิยามนี้

ประเด็นพิจารณา	แนวทางปฏิบัติที่ดี
ภัยอันตราย	กรอบการทำงานด้านการคุ้มครองข้อมูลควรปรับเปลี่ยนการคุ้มครองให้เหมาะสมกับความเสี่ยงภัยอันตรายที่อาจจะเกิดขึ้นกับผู้บริโภค ภัยอันตรายที่ระบุได้อย่างชัดเจนควรสะท้อนให้เห็นภาพการบาดเจ็บทางร่างกาย ผลกระทบต่อสุขภาพอย่างร้ายแรง ความเสียหายทางการเงิน หรือการเปิดเผยข้อมูลส่วนบุคคลที่มีลักษณะอ่อนไหว ซึ่งอยู่นอกเหนือความคาดหวังของผู้บริโภคและจะก่อให้เกิดผลเสียหายร้ายแรงตามมาอย่างเป็นรูปธรรม
ความโปร่งใส	ผู้ควบคุมข้อมูลควรให้คำอธิบายที่ชัดเจนและเข้าใจได้ เกี่ยวกับแนวทางปฏิบัติในการจัดการข้อมูลส่วนบุคคล ซึ่งรวมถึงหมวดหมู่ของข้อมูลส่วนบุคคลที่เก็บ ประเภทของบุคคลที่สามที่ผู้ควบคุมข้อมูลจะส่งต่อข้อมูลให้ไป และคำอธิบายเกี่ยวกับขั้นตอนที่ผู้ควบคุมข้อมูลจะดำเนินการอย่างต่อเนื่องเพื่อตรวจสอบ ขั้นตอนการร้องขอการเปลี่ยนแปลงข้อมูลส่วนบุคคล ขั้นตอนการร้องขอสำเนาของข้อมูลส่วนบุคคล หรือขั้นตอนการลบข้อมูลส่วนบุคคล
การระบุวัตถุประสงค์	ข้อมูลส่วนบุคคลควรเกี่ยวข้องกับวัตถุประสงค์ในการเก็บและได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าว โดยวิธีที่ชอบด้วยกฎหมาย ผู้ควบคุมข้อมูลควรแจ้งให้ผู้บริโภคทราบเรื่องวัตถุประสงค์ในการเก็บข้อมูลส่วนบุคคล และควรใช้ข้อมูลส่วนบุคคลในลักษณะที่สอดคล้องกับคำอธิบาย บริบทของธุรกรรม หรือสอดคล้องกับความคาดหวังอันควรของผู้บริโภค หรือในลักษณะอื่นที่สอดคล้องกับวัตถุประสงค์เดิมในการเก็บข้อมูล ผู้ควบคุมข้อมูลควรใช้ระบบกำกับดูแลที่ทำให้ยืนยันได้ว่าการใช้และส่งต่อข้อมูลส่วนบุคคล เป็นไปในลักษณะที่สอดคล้องกับวัตถุประสงค์ที่กำหนดไว้
คุณภาพของข้อมูล	ข้อมูลส่วนบุคคลควรเกี่ยวข้องกับวัตถุประสงค์ในการนำไปใช้ และควรมีความถูกต้อง ครบถ้วนและเป็นปัจจุบัน ในขอบเขตที่จำเป็นสำหรับการบรรลุวัตถุประสงค์ดังกล่าว
เหตุผลของการประมวลผล	กรอบการทำงานด้านการคุ้มครองข้อมูลควรยอมรับการประมวลผลข้อมูล และยอมให้มีการดำเนินการเพื่อประมวลผลข้อมูลในขอบเขตของเหตุผลอันควร ซึ่งได้แก่ เพื่อบรรลุวัตถุประสงค์ทางธุรกิจที่ชอบด้วยกฎหมาย ซึ่งสอดคล้องกับบริบทของธุรกรรม หรือสอดคล้องกับความคาดหวังของผู้บริโภค วัตถุประสงค์ที่สมเหตุสมผลอื่น ๆ ประกอบด้วยการปฏิบัติตามสัญญา เพื่อสาธารณประโยชน์หรือผลประโยชน์ที่สำคัญสูงสุดของผู้บริโภค การปฏิบัติตามข้อผูกพันตามกฎหมาย หรือการปฏิบัติตามความยินยอมของผู้บริโภค กรอบการทำงานด้านการคุ้มครองข้อมูลไม่ควรจำกัดความพยายามขององค์กรในการรักษาความปลอดภัยทางไซเบอร์ที่เป็นไปตามกฎหมาย การดำเนินมาตรการเพื่อตรวจจับหรือป้องกันการฉ้อโกงหรือการโจรกรรมเอกลักษณ์บุคคล ความสามารถในการคุ้มครองข้อมูลลับ หรือการดำเนินการหรือป้องกันการอ้างสิทธิ์ตามกฎหมาย
การยินยอม	ผู้ควบคุมข้อมูลควรช่วยผู้บริโภคให้มีความสามารถในการตัดสินใจเลือก โดยการให้ข้อมูล และช่วยให้ผู้บริโภคสามารถยกเลิกการประมวลผลข้อมูลส่วนบุคคลของตนได้ ในกรณีที่กระทำได้และเหมาะสม ในสถานการณ์ที่ควรมีการให้ความยินยอม ความยินยอมควรให้เมื่อถึงเวลาและในรูปแบบที่เกี่ยวข้องกับบริบทของการทำธุรกรรมหรือบริบทของความสัมพันธ์ระหว่างองค์กรกับผู้บริโภค
การประมวลผลข้อมูลส่วนบุคคลที่อ่อนไหว	ข้อมูลบางอย่าง เช่น ข้อมูลบัญชีการเงิน หรือเงื่อนไขทางสุขภาพ อาจมีความอ่อนไหวเป็นพิเศษ หากการประมวลผลข้อมูลที่อ่อนไหวแสดงให้เห็นความเสี่ยงในระดับสูง ที่จะเกิดภัยอันตรายต่อความเป็นส่วนตัว ผู้ควบคุมข้อมูลควรเปิดโอกาสให้ผู้บริโภคแสดงการยินยอมอย่างชัดแจ้ง

ประเด็นพิจารณา	แนวทางปฏิบัติที่ดี
การควบคุมโดยผู้บริโภค	ผู้บริโภคควรจะสามารถขอข้อมูลเพื่อแสดงให้เห็นว่าองค์กรมีข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตน และมีข้อมูลในลักษณะดังกล่าวหรือไม่ ผู้บริโภคควรจะสามารถตั้งคำถามเกี่ยวกับความถูกต้องของข้อมูลนั้น และแก้ไขหรือลบข้อมูลได้ตามความเหมาะสม ผู้บริโภคยังควรจะสามารถขอรับสำเนาของข้อมูลส่วนบุคคลที่ให้ไว้กับองค์กร หรือข้อมูลที่ผู้บริโภคสร้างขึ้นเองได้ องค์กรควรมีความยืดหยุ่นในการกำหนดวิธีและรูปแบบที่เหมาะสมในการจัดเตรียมข้อมูลให้แก่ผู้บริโภค ผู้ควบคุมข้อมูล ซึ่งมีหน้าที่กำหนดวิธีและวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล ควรมีหน้าที่รับผิดชอบหลักในการตอบสนองต่อคำขอที่เกี่ยวข้องกับเรื่องเหล่านี้ ผู้ควบคุมข้อมูลอาจปฏิเสธคำขอดังกล่าวได้ ในกรณีที่ภาระหรือค่าใช้จ่ายของการดำเนินการเช่นนั้นไม่สมเหตุสมผล หรือไม่ได้สัดส่วนกับภัยอันตรายที่อาจจะเกิดขึ้นกับความเป็นส่วนตัวของผู้บริโภค ในกรณีที่ต้องปฏิบัติตามข้อกำหนดทางกฎหมาย ในกรณีที่การดำเนินการตามคำขอดังกล่าวอาจจะกระทบต่อความปลอดภัยของเครือข่าย หรือในกรณีที่เป็นการฝ่าฝืนการคุ้มครองข้อมูลลับทางการค้า ในกรณีเพื่อให้เป็นไปตามวัตถุประสงค์ทางการวิจัย หรือในกรณีเพื่อให้เป็นไปตามวัตถุประสงค์ที่ต้องการจะหลีกเลี่ยงการละเมิดความเป็นส่วนตัว หลีกเลี่ยงการละเมิดเสรีภาพในการ พูด หรือหลีกเลี่ยงการละเมิดสิทธิอื่น ๆ ของผู้บริโภค นอกจากนี้ ผู้ควบคุมข้อมูลควรดำเนินการตามขั้นตอนการตรวจสอบความปลอดภัย เพื่อยืนยันตัวตนของผู้บริโภคที่ส่งคำร้องขอ เพื่อลดความเสี่ยงภัยอันตรายจากการเปิดเผยข้อมูลที่ไม่เหมาะสม
การแจ้งเตือนเรื่องการละเมิดและการรักษาความปลอดภัย	ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลควรใช้มาตรการด้านความปลอดภัยที่สมเหตุสมผลและเหมาะสมซึ่งสอดคล้องกับปริมาณและความอ่อนไหวของข้อมูล ขนาด และความซับซ้อนของธุรกิจ และต้นทุนของเครื่องมือที่ใช้งานซึ่งออกแบบมาเพื่อป้องกันการเข้าถึง การทำลาย การใช้ การดัดแปลงแก้ไข และการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต ผู้ควบคุมข้อมูลควรแจ้งให้ผู้บริโภคทราบให้เร็วที่สุดเท่าที่จะทำได้ในทางปฏิบัติ ภายหลังพบการละเมิดข้อมูลส่วนบุคคล ในลักษณะที่เกี่ยวข้องกับการได้มาโดยไม่ได้รับอนุญาตซึ่งข้อมูลส่วนบุคคลที่ไม่ได้เข้ารหัส หรือไม่ได้ถูกปกปิดเนื้อหาบางส่วนเพื่อวัตถุประสงค์ด้านความปลอดภัย ซึ่งการละเมิดดังกล่าวอาจทำให้เกิดความเสี่ยงอย่างมีนัยสำคัญ ที่จะส่งผลให้เกิดการโจรกรรมเอกลักษณ์บุคคลหรือการฉ้อโกงทางการเงิน ผู้ควบคุมข้อมูลอาจรายงานการละเมิดไปยังหน่วยงานที่กำกับดูแลอย่างสม่ำเสมอ รวมทั้งรายงานมาตรการรักษาความปลอดภัยที่องค์กรมีการดำเนินการ ซึ่งเป็นส่วนหนึ่งของข้อกำหนดด้านภาระความรับผิดชอบ
ข้อกำหนดด้านภาระความรับผิดชอบ	ผู้ควบคุมข้อมูลควรพัฒนานโยบายและกระบวนการดังต่อไปนี้ เพื่อป้องกันภัยอันตราย ได้แก่ มอบหมายให้บุคคลประสานงานการดำเนินการตามขั้นตอนและกระบวนการ เพื่อป้องกันภัยอันตราย และจัดให้มีการฝึกอบรมและการบริหารจัดการสำหรับพนักงาน จัดให้มีการติดตามและประเมินผลการดำเนินการตามขั้นตอนและกระบวนการ เพื่อป้องกันภัยอันตรายเป็นประจำ ตลอดจนปรับเปลี่ยนแนวทางปฏิบัติ เพื่อแก้ไขปัญหาที่เกิดขึ้นตามที่จำเป็น ตามมาตรการดังกล่าว ผู้ควบคุมข้อมูลอาจดำเนินการประเมินความเสี่ยงเป็นระยะ ในขณะที่ประมวลผลข้อมูลที่ลักษณะอ่อนไหว และเมื่อพบความเสี่ยงอย่างมีนัยสำคัญที่จะส่งผลให้เกิดภัยอันตราย ให้ทำการบันทึกการดำเนินการตามขั้นตอนและกระบวนการอย่างเหมาะสม เพื่อป้องกันภัยอันตรายดังกล่าว รัฐบาลไม่ควรมีข้อกำหนดให้ต้องรายงานผลการประเมินความเสี่ยง หรือต้องขอคำปรึกษากับองค์กรที่มีหน้าที่กำกับดูแลก่อนล่วงหน้า เนื่องจากข้อกำหนดดังกล่าวจะสร้างภาระในการดำเนินการที่ไม่จำเป็น และส่งผลให้เกิดความล่าช้าในการดำเนินการเพื่อให้บริการ และไม่ได้เกิดประโยชน์ทางด้านการคุ้มครองความเป็นส่วนตัวแต่อย่างใด

ประเด็นพิจารณา	แนวทางปฏิบัติที่ดี
การเคลื่อนย้ายของข้อมูลข้ามพรมแดน	กรอบการทำงานด้านการคุ้มครองข้อมูลควรส่งเสริมและสนับสนุนให้เกิดการเคลื่อนย้ายของข้อมูล ซึ่งจะช่วยผลักดันการเติบโตของเศรษฐกิจโลก องค์กรที่ต้องเคลื่อนย้ายข้อมูลไปทั่วโลกควรดำเนินการตามกระบวนการที่ทำให้ยืนยันได้ว่าข้อมูลที่มีการเคลื่อนย้ายออกนอกประเทศ ยังคงได้รับการคุ้มครองอย่างต่อเนื่อง ในกรณีที่แนวทางการคุ้มครองข้อมูลมีความแตกต่างกัน รัฐบาลควรสร้างเครื่องมือเพื่อประสานความแตกต่างเหล่านั้น ในลักษณะที่ส่งเสริมทั้งการคุ้มครองความเป็นส่วนตัว และส่งเสริมการเคลื่อนย้ายของข้อมูล กรอบการทำงานด้านการคุ้มครองข้อมูลควรห้ามไม่ให้มีการกำหนดเงื่อนไขในลักษณะบังคับให้ทั้งภาครัฐและภาคเอกชนต้องจัดเก็บข้อมูลไว้ภายในประเทศ ซึ่งการกำหนดเงื่อนไขดังกล่าว อาจเป็นอุปสรรคต่อความพยายามในการดำเนินมาตรการรักษาความปลอดภัยของข้อมูล ขัดขวางนวัตกรรมทางธุรกิจ และจำกัดขอบเขตของบริการที่มีให้กับผู้บริโภค
หน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล / การจัดสรรความรับผิด	ผู้ควบคุมข้อมูล ซึ่งมีหน้าที่กำหนดวิธีและวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล ควรมีหน้าที่รับผิดชอบหลักในเรื่องการปฏิบัติตามกฎหมายเรื่องการคุ้มครองความเป็นส่วนตัวและการรักษาความปลอดภัย ผู้ประมวลผลข้อมูล ซึ่งมีหน้าที่ประมวลผลข้อมูลเพื่อประโยชน์ของผู้ควบคุมข้อมูล ควรมีหน้าที่รับผิดชอบเฉพาะในเรื่องการปฏิบัติตามคำสั่งของผู้ควบคุมข้อมูล ภายในขอบเขตของข้อตกลงตามที่ระบุไว้ในสัญญาเท่านั้น ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลควรมีโอกาสที่จะเจรจาต่อรองข้อกำหนดในสัญญาที่พวกเขากำหนดให้มีขึ้นกับบุคคลอื่นเอง โดยไม่ถูกบังคับให้ใช้ภาษาที่กฎหมายกำหนด
การเยียวยาและการลงโทษ	ผู้กำกับดูแลควรมีเครื่องมือและทรัพยากรที่จำเป็น เพื่อทำให้ยืนยันได้ว่าการบังคับใช้กฎหมายเป็นไปอย่างมีประสิทธิภาพ การเยียวยาและการลงโทษควรเป็นไปตามสัดส่วนกับความเสียหาย ที่เป็นผลมาจากการละเมิดกฎหมายคุ้มครองข้อมูล การลงโทษทางแพ่งไม่ควรถูกกำหนดขึ้นโดยพลการหรือตามปัจจัยที่ขาดความเชื่อมโยงอย่างมีสาระสำคัญกับบริบทซึ่งความเสียหายได้เกิดขึ้น การลงโทษทางอาญาไม่ใช่การเยียวยาที่เหมาะสม ในกรณีการละเมิดกฎหมายคุ้มครองข้อมูล